CLAIMS

What is claimed is:

1. A system to uniquely identify a security device, the security device coupled to a computing device, the computing device coupled to a server over a computer network, the system comprising:

a security device coupled to the computing device, the security device storing a serial number associated with the security device and a user key associated with the serial number;

a server coupled to a user information database, the user information database storing a plurality of registered serial numbers and a plurality of user keys, each user key being associated with one of the plurality of registered serial numbers;

wherein, when the computing device attempts to log onto the server over the computer network, the server:

requests a serial number from the security device;

verifies whether the serial number received from the security device is stored as one of the plurality of registered serial numbers in the user information database;

if the serial number is stored within the user information database, the server obtains the associated user key and computes a challenge and computes an expected response based on the associated user key, the server sends the challenge to the security device over the computer network; and

if the server receives a response back from the security device in response to the challenge that matches the expected response, the server allows the computing device to log onto the server.

2. The system of claim 1, wherein the serial number and the user key are sealed in a secure memory of the security device.

3. The system of claim 1, wherein the security device further comprises a microprocessor and a security device memory.

4. The system of claim 1, wherein the expected response computed at the server and the response computed at the security device, are both based on a one-way hashing function of the user key and the challenge.

5. The system of claim 1, wherein the server updates the current date at the security device and updates an expiration date at the security device.

6. The system of claim 1, wherein the server unlocks a security device memory of the security device.

7. The system of claim 6, wherein unlocking the security device memory of the security device includes the server computing a memory unlock message based upon a memory key associated with the serial number of the security device stored at the server, sending the memory unlock message to the security device, and if the security device verifies the memory unlock message as being valid, the security device unlocks the security device memory.

8. The system of claim 7, wherein the server locks the security device memory by sending a memory lock command to the security device.

9. The system of claim 1, wherein the server encrypts an asset with an asset key and sends the encrypted asset to the computing device, the computing device storing the encrypted asset.

10. The system of claim 9, wherein the server encrypts the asset key with the user key and sends the encrypted asset key to the computing device, the computing device storing the encrypted asset key.

11. The system of claim 10, wherein encrypting the asset key with the user key further comprises encrypting a rental flag identifying whether the associated asset is to be rented or purchased.

12. The system of claim 10, wherein the security device decrypts the asset key that is encrypted with the user key using the user key stored by the security device.

13. The system of claim 12, wherein the security device transmits the decrypted asset key to the computing device such that the computing device uses the decrypted asset key to decrypt the asset.

14. A method to uniquely identify a security device, the security device coupled to a computing device, the computing device coupled to a server over a computer network, the method comprising:

storing a serial number associated with the security device and a user key associated with the serial number at the security device;

storing a plurality of registered serial numbers and a plurality of user keys at the server, each user key being associated with one of the plurality of registered serial numbers;

requesting a serial number from the security device when the computing device attempts to log onto the server over the computer network;

verifying whether the serial number received from the security device is stored as one of the plurality of registered serial numbers at the server;

if the serial number is stored at the server,

obtaining the associated user key from the server;

computing a challenge;

computing an expected response based on the associated user key;

sending the challenge to the security device over the computer network; and

if the server receives a response back from the security device in response to the challenge that matches the expected response, allowing the computing device to log onto the server.

15. The method of claim 14, wherein the serial number and the user key are sealed in a secure memory of the security device.

16. The method of claim 14, wherein the security device comprises a microprocessor and a security device memory.

17. The method of claim 14, wherein the expected response is computed at the server and the response is computed at the security device, both the response and the expected response being based on a one-way hashing function of the user key and the challenge.

18. The method of claim 14, further comprising updating the current date and an expiration date at the security device.

19. The method of claim 14, further comprising unlocking a security device memory of the security device.

20. The method of claim 19, wherein unlocking the security device memory of the security device includes computing a memory unlock message based upon a memory key associated with the security device, sending the memory unlock message to the security device, and if the security device verifies the memory unlock message as being valid, unlocking the security device memory.

21. The method of claim 20, further comprising locking the security device memory by sending a memory lock command to the security device.

22. The method of claim 14, further comprising encrypting an asset with an asset key and sending the encrypted asset to the computing device, the computing device storing the encrypted asset.

23. The method of claim 22, wherein the asset key is encrypted with the user key and the encrypted asset key is sent to the computing device, the computing device storing the encrypted asset key.

24. The method of claim 23, wherein encrypting the asset key with the user key further comprises encrypting a rental flag identifying whether the associated asset is to be rented or purchased.

25. The method of claim 23, wherein the security device decrypts the asset key that is encrypted with the user key using the user key stored by the security device.

26. The method of claim 25, wherein the security device transmits the decrypted asset key to the computing device such that the computing device uses the decrypted asset key to decrypt the asset.

27. A security device to uniquely identify and authenticate a user, the security device coupled to a computing device, the computing device coupled to a server over a computer network, the server coupled to a user information database, the user information database storing a plurality of registered serial numbers and a plurality of user keys, each user key being associated with one of the plurality of registered serial numbers, the security device comprising:

a microprocessor; and

a security device memory, the security device memory storing a serial number associated with the security device and a user key associated with the serial number;

wherein, when the computing device attempts to log onto the server over the computer network, the microprocessor operating in conjunction with the security device memory to:

in response to a request from the sever, transmit the serial number to the computing device which is then transmitted to the server;

in response to a challenge from the server, compute a response based upon the user key; and

transmit the response to the computing device which is then transmitted to the server.

28. The security device of claim 27, wherein the serial number and the user key are sealed in a secure memory of the security device.

29. The security device of claim 27, wherein the response computed at the security device is based on a one-way hashing function of the user key and the challenge.

30. The security device of claim 27, wherein the server encrypts an asset with an asset key and sends the encrypted asset to the computing device, the computing device storing the encrypted asset, and further the server encrypts the asset key with the user key and sends the encrypted asset key to the computing device, the computing device transmitting the encrypted asset key to the security device.

31. The security device of claim 30, wherein the microprocessor operating in conjunction with the security device memory decrypts the asset key that is encrypted with the user key using the user key stored in the security device memory.

32. The security device of claim 31, further comprising transmitting the decrypted asset key to the computing device such that the computing device uses the decrypted asset key to decrypt the asset.

33. A system to uniquely identify a security device, the security device coupled to a computing device, the computing device coupled to a server over a computer network, the system comprising:

a security device coupled to the computing device, the security device storing a unique identifier associated with the security device and a user key associated with the unique identifier;

a server coupled to a user information database, the user information database storing a plurality of registered unique identifiers and a plurality of user keys, each user key being associated with one of the plurality of registered unique identifiers;

wherein, when the computing device attempts to log onto the server over the computer network, the server:

requests a unique identifier from the security device;

verifies whether the unique identifier received from the security device is stored as one of the plurality of registered unique identifiers in the user information database;

if the unique identifier is stored within the user information database, the server obtains the associated user key and computes a challenge and computes an expected response based on the associated user key, the server sends the challenge to the security device over the computer network; and

if the server receives a response back from the security device in response to the challenge that matches the expected response, the server allows the computing device to log onto the server.

34. The system of claim 33, wherein the unique identifier and the user key are sealed in a secure memory of the security device.

35. The system of claim 34, wherein the unique identifier is a serial number.

36. The system of claim 33, wherein the security device further comprises a microprocessor and a security device memory.

37. The system of claim 33, wherein the expected response computed at the server and the response computed at the security device, are both based on a one-way hashing function of the user key and the challenge.

38. The system of claim 33, wherein the server updates the current date at the security device and updates an expiration date at the security device.

39. The system of claim 33, wherein the server unlocks a security device memory of the security device.

40. The system of claim 39, wherein unlocking the security device memory of the security device includes the server computing a memory unlock message based upon a memory key associated with the unique identifier of the security device stored at the server, sending the memory unlock message to the security device, and if the security device verifies the memory unlock message as being valid, the security device unlocks the security device memory.

41. The system of claim 40, wherein the server locks the security device memory by sending a memory lock command to the security device.

42. The system of claim 33, wherein the server encrypts an asset with an asset key and sends the encrypted asset to the computing device, the computing device storing the encrypted asset.

43. The system of claim 42, wherein the server encrypts the asset key with the user key and sends the encrypted asset key to the computing device, the computing device storing the encrypted asset key.

44. The system of claim 43, wherein encrypting the asset key with the user key further comprises encrypting a rental flag identifying whether the associated asset is to be rented or purchased.

45. The system of claim 43, wherein the security device decrypts the asset key that is encrypted with the user key using the user key stored by the security device.

46. The system of claim 45, wherein the security device transmits the decrypted asset key to the computing device such that the computing device uses the decrypted asset key to decrypt the asset.